REMARKS

Upon entry of this amendment, claims 14-21 are all the claims pending in the application. Claims 1-13 have been canceled by this amendment, and claims 14-21 have been added as new claims. No new matter has been added.

I. Claim Rejections

Claims 1, 8 and 11 have been rejected under 35 U.S.C. § 102(b) as being anticipated by Hori et al. (US 2002/0184154); and claims 2-7, 9, 10, 12 and 13 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over Hori et al.

As noted above, claims 1-13 have been canceled and are replaced with new claims 14-21 in order to further distinguish the claimed invention from the Hori reference applied by the Examiner. In this regard, Applicants submit that the above-noted rejections based on Hori are inapplicable to the new claims for at least the following reasons.

Regarding claim 14, Applicants note that this claim recites the feature of a digital signature management unit configured to (i) generate a hash value of the encrypted information before the encrypted information is stored into the storage unit, and hold the generated hash value, and (ii) verify validity of the encrypted information by reading the encrypted information stored in the storage unit, generating a hash value of the read encrypted information, and comparing the generated hash value of the encrypted information before the encrypted information is stored into the storage unit with the generated hash value of the read encrypted information, the validity indicating that the encrypted information has not been tampered with.

Applicants respectfully submit that Hori does not teach, suggest or otherwise render obvious at least the above-noted feature recited in new claim 14.

In particular, with respect to Hori, Applicants note that this reference teaches a distribution system in which a distribution of a decryption key from a server to a memory card can be resumed, and the rights of the copyright owners can also be protected, even when a communication for the distribution of the decryption key is interrupted between the server and the memory card before the distribution of the decryption key is completed. In this regard, Applicants note that Hori discloses the use of a controller 1420 in a memory card 110, the controller having the ability to calculate a hash value of encrypted data by encrypting status information in which a status flag is added to a reception log held in a log memory 1460 (see paragraphs [0219] through [0222]).

Based on the foregoing description, Applicants note that while Hori discloses the ability to calculate a hash value of encrypted data by encrypted status information, that Hori does not disclose, suggest or render obvious the above-noted feature recited in claim 14 of a digital signature management unit configured to (i) generate a hash value of the encrypted information before the encrypted information is stored into the storage unit, and hold the generated hash value, and (ii) verify validity of the encrypted information by reading the encrypted information stored in the storage unit, generating a hash value of the read encrypted information, and comparing the generated hash value of the encrypted information before the encrypted information is stored into the storage unit with the generated hash value of the read encrypted information, the validity indicating that the encrypted information has not been tampered with.

Accordingly, Applicants respectfully submit that new claim 14 is patentable over Hori, an indication of which is kindly requested.

It is noted that by providing the above-noted feature recited in claim 14, it is possible to reduce memory capacity to be held in a tamper resistance module and prevent fraud such as tampering with and replacement of encrypted information stored in a storage unit not having tamper resistance, by storing the encrypted information in the storage unit not having tamper resistance, and by holding a hash value of the encrypted information in the tamper resistance module.

Regarding claims 15-19, Applicants note that these claims depend from claim 14 and are therefore considered patentable at least by virtue of their dependency.

Regarding claims 20 and 21, Applicants note that each of these claims recites the feature of a digital signature management step of (i) generating and holding a hash value of the encrypted information before the encrypted information is stored into the storage unit and (ii) verifying validity of the encrypted information by reading the encrypted information stored in the storage unit, generating a hash value of the read encrypted information, and comparing the generated hash value of the encrypted information before the encrypted information is stored into the storage unit with the generated hash value of the read encrypted information, the validity indicating that the encrypted information has not been tampered with.

For at least similar reasons as discussed above with respect to claim 14, Applicants respectfully submit that Hori does not disclose, suggest or otherwise render obvious the above-noted feature recited in claims 20 and 21. Accordingly, Applicants submit that claims 20 and 21

are patentable over Hori, an indication of which is kindly requested.

II. Conclusion

In view of the above, reconsideration and allowance of this application are now believed to be in order, and such actions are hereby solicited. If any points remain in issue which the Examiner feels may best be resolved through a personal or telephone interview, the Examiner is kindly requested to contact the undersigned at the telephone number listed below.

The Commissioner is authorized to charge any deficiency or to credit any overpayment associated with this communication to Deposit Account No. 23-0975.

Respectfully submitted,

Motoji OHMORI et al.

/Kenneth W. Fields/
By: 2009.07.13 12:48:32 -04'00'
Kenneth W. Fields
Registration No. 52,430
Attorney for Applicants

KWF/krg
Washington, D.C. 20005-1503
Telephone (202) 721-8200
Facsimile (202) 721-8250
July 13, 2009